AMENDMENTS TO THE CLAIMS:

Please cancel without prejudice claims 3, 9, 17, 23, 31 and 37 and amend claims 1, 5, 7, 11, 15, 19, 21, 25, 29, 33, 35 and 39 as follows.

This listing of claims will replace all prior versions, and listings, of claims in the application:

1. (currently amended) A computer program product comprising a computer program operable to control a computer to generate banned program identifying data indicative of <u>at least</u> one ~~or more~~ computer programs to be banned from use, said computer <u>controlling</u> program comprising:

(i)   user controlled program specifying logic operable to specify <u>said at least</u> one ~~or more~~ computer programs to be banned from use<u>, said at least one computer program comprising an undesired, non-virus computer program</u>; and

(ii)   banned program identifying data generating logic responsive to said user controlled program specifying logic to generate banned program identifying data for said <u>at least</u> one ~~or more~~ computer programs to be banned from use, said banned program identifying data being operable to control anti computer virus logic to identify computer programs banned from use.

2. (original) A computer program product as claimed in claim 1, wherein said banned program identifying data is encrypted with a private key.

3. (cancelled).

4. (original) A computer program product as claimed in claim 1, wherein said banned

program identifying data controls said anti computer virus logic to identify said computer

programs banned from use in a manner substantially the same as if they were a computer virus.

5. (currently amended) A computer program product as claimed in claim 4, wherein said

banned program identifying data includes heuristic data identifying at least one or more

behavioural characteristics of at least one or more computer programs banned from use such that

variants of said at least one or more computer programs banned from use that share said

behavioural characteristics may also be identified.

6. (original) A computer program product as claimed in claim 1, wherein said banned

program identifying data comprises data identifying permitted computer programs with all

computer programs not matching a permitted computer program being identified as a computer

program banned from use.

7. (currently amended) A computer program product comprising a computer program

operable to control a computer to ban from use at least one or more computer programs, said at

least one computer program comprising an undesired, non-virus computer program, said

computer program comprising:

(i)   anti computer virus logic responsive to user generated banned program

identifying data for said at least one or more computer programs to be banned from use to

identify computer programs banned from use.

8. (original) A computer program product as claimed in claim 7, wherein said banned program identifying data is encrypted with a private key and said anti computer virus logic uses a corresponding public key to decrypt said user generated banned program identifying data prior to use.

9. (cancelled).

10. (original) A computer program product as claimed in claim 8, wherein said decrypted banned program identifying data is stored within a secured memory region once decrypted.

11. (currently amended) A computer program product as claimed in claim 7, wherein when a banned computer program is identified, at least one or more banned program actions are is triggered, said banned program actions comprising at least one of:

    (i)   issuing an alert message indicating identification of a banned computer program;

    (ii)   denying access to said banned computer program;

    (iii)   encrypting said banned computer program; and

    (iv)   deleting said banned computer program.

12. (original) A computer program product as claimed in claim 7, wherein said anti computer virus logic responses to an absence of said user generated banned program identifying data by performing at least one of:

(i)   issuing an alert message indicating an absence of said user generated banned

program identifying data;

(ii)   restoring said user generated banned program identifying data from a remote

source;

(iii)   disabling a computer upon which said anti computer virus logic is executing.

13. (original) A computer program product as claimed in claim 7, wherein said anti

computer virus logic is executable as a separate instance solely to identify computer programs

banned from use.

14. (original) A computer program product as claimed in claim 7, wherein said user

generated banned program identifying data comprises data identifying permitted computer

programs with all computer programs not matching a permitted computer program being

identified as a computer program banned from use.

15. (currently amended) A method of generating banned program identifying data

indicative of at least one or more computer programs to be banned from use, said method

comprising the steps of:

(i)   user specifying at least one or more computer programs to be banned from use,

said at least one computer program comprising an undesired, non-virus computer program; and

(ii)   generating banned program identifying data for said at least one or more computer

programs to be banned from use, said banned program identifying data being operable to control

anti computer virus logic to identify computer programs banned from use.

16. (original) A method as claimed in claim 15, wherein said banned program identifying data is encrypted with a private key.

17. (cancelled).

18. (original) A method as claimed in claim 15, wherein said banned program identifying data controls said anti computer virus logic to identify said computer programs banned from use in a manner substantially the same as if they were a computer virus.

19. (currently amended) A method as claimed in claim 18, wherein said banned program identifying data includes heuristic data identifying at least one or more behavioural characteristics of at least one or more computer programs banned from use such that variants of said at least one or more computer programs banned from use that share said behavioural characteristics may also be identified.

20. (original) A method as claimed in claim 15, wherein said banned program identifying data comprises data identifying permitted computer programs with all computer programs not matching a permitted computer program being identified as a computer program banned from use.

21. (currently amended) A method for banning from use at least one ~~or more~~ computer programs, said at least one computer program comprising an undesired, non-virus computer program, said method comprising the step of:

(i)   in response to user generated banned program identifying data for said at least one ~~or more~~ computer programs to be banned from use, operating anti computer virus logic to identify computer programs banned from use.

22. (original) A method as claimed in claim 21, wherein said banned program identifying data is encrypted with a private key and said anti computer virus logic uses a corresponding public key to decrypt said user generated banned program identifying data prior to use.

23. (cancelled).

24. (original) A method as claimed in claim 22, wherein said decrypted banned program identifying data is stored within a secured memory region once decrypted.

25. (currently amended) A method as claimed in claim 21, wherein when a banned computer program is identified, at least one ~~or more~~ banned program actions ~~are~~ is triggered, said banned program actions comprising at least one of:

(i)   issuing an alert message indicating identification of a banned computer program;

(ii)   denying access to said banned computer program;

(iii)   encrypting said banned computer program; and

(iv)   deleting said banned computer program.

910488

26. (original) A method as claimed in claim 21, wherein said anti computer virus logic responses to an absence of said user generated banned program identifying data by performing at least one of:

(i)   issuing an alert message indicating an absence of said user generated banned program identifying data;

(ii)   restoring said user generated banned program identifying data from a remote source;

(iii)   disabling a computer upon which said anti computer virus logic is executing.

27. (original) A method as claimed in claim 21, wherein said anti computer virus logic is executable as a separate instance solely to identify computer programs banned from use.

28. (original) A method as claimed in claim 21, wherein said banned program identifying data comprises data identifying permitted computer programs with all computer programs not matching a permitted computer program being identified as a computer program banned from use.

29. (currently amended) Apparatus for generating banned program identifying data indicative of <u>at least</u> one ~~or more~~ computer programs to be banned from use, said apparatus comprising:

(i) a user controlled program specifier operable to specify <u>at least</u> one ~~or more~~

computer programs to be banned from use<u>, said at least one computer program comprising an

undesired, non-virus computer program</u>; and

(ii) banned program identifying data generator responsive to said user controlled

program specifier to generate banned program identifying data for said <u>at least</u> one ~~or more~~

computer programs to be banned from use, said banned program identifying data being operable

to control anti computer virus logic to identify computer programs banned from use.

30. (original) Apparatus as claimed in claim 29, wherein said banned program identifying

data is encrypted with a private key.

31. (cancelled).

32. (original) Apparatus as claimed in claim 29, wherein said banned program identifying

data controls said anti computer virus logic to identify said computer programs banned from use

in a manner substantially the same as if they were a computer virus.

33. (currently amended) Apparatus as claimed in claim 32, wherein said banned program

identifying data includes heuristic data identifying <u>at least</u> one ~~or more~~ behavioural

characteristics of <u>at least</u> one ~~or more~~ computer programs banned from use such that variants of

said <u>at least</u> one ~~or more~~ computer programs banned from use that share said behavioural

characteristics may also be identified.

34. (original) Apparatus as claimed in claim 29, wherein said banned program identifying

data comprises data identifying permitted computer programs with all computer programs not

matching a permitted computer program being identified as a computer program banned from

use.

35. (currently amended) Apparatus for banning from use at least one or more computer

programs, said at least one computer program comprising an undesired, non-virus computer

program, said apparatus comprising:

(i)   an anti computer virus system responsive to user generated banned program

identifying data for said at least one or more computer programs to be banned from use to

identify computer programs banned from use.

36. (original) Apparatus as claimed in claim 35, wherein said banned program identifying

data is encrypted with a private key and said anti computer virus logic uses a corresponding

public key to decrypt said user generated banned program identifying data prior to use.

37. (cancelled).

38. (original) Apparatus as claimed in claim 36, wherein said decrypted banned program

identifying data is stored within a secured memory region once decrypted.

910488

39. (currently amended) Apparatus as claimed in claim 35, wherein when a banned computer program is identified, <u>at least</u> one ~~or more~~ banned program actions ~~are~~ <u>is</u> triggered, said banned program action~~s~~ comprising at least one of:

    (i)   issuing an alert message indicating identification of a banned computer program;

    (ii)   denying access to said banned computer program;

    (iii)   encrypting said banned computer program; and

    (iv)   deleting said banned computer program.

40. (original) Apparatus as claimed in claim 35, wherein said anti computer virus system responses to an absence of said user generated banned program identifying data by performing at least one of:

    (i)   issuing an alert message indicating an absence of said user generated banned program identifying data;

    (ii)   restoring said user generated banned program identifying data from a remote source;

    (iii)   disabling a computer upon which said anti computer virus logic is executing.

41. (original) Apparatus as claimed in claim 35, wherein said anti computer virus system is executable as a separate instance solely to identify computer programs banned from use.

42. (original) Apparatus as claimed in claim 35, wherein said user generated banned program identifying data comprises data identifying permitted computer programs with all

computer programs not matching a permitted computer program being identified as a computer

program banned from use.